Setting up Parallels RAS to work with Azure Identity Provider over SAML

- Parallels Remote Application Server 18.0
- Parallels Remote Application Server 18.1
- Parallels Remote Application Server 19.1
- Parallels Remote Application Server 18.3
- Parallels Remote Application Server 18.2
- Parallels Remote Application Server 19.0

This article is a step-by-step guide to configure single sign-on (SSO) Authentication using the Security Assertion Markup Language (SAML) authentication mechanism. SAML is an XML-based authentication mechanism that provides SSO capability between different organizations by allowing the user authentication without sharing the local identity database. As part of the SAML SSO process, the new Parallels® Remote Application Server (RAS) Enrollment Server communicates with Microsoft Certificate Authority (CA) to request, enroll and manage digital certificates on behalf of the user to complete authentication without requiring the users to put in their Active Directory (AD) credentials.

Service providers and enterprises with multiple subsidiaries (acquisitions) don't have to maintain their own internal identity management solutions or complex domains or forest trusts. Integrating with a third-party identity providers (IdP) allows customers' and partners' end users to have a true SSO experience.

As an example, we will review the process of configuring Azure as identity provider.

Prerequisites

1. Local Active Directory:

- A local AD user account for use as enrollment agent (CA terminology)
- A local AD limited user account for Network Level Authentication (NLA) authentication.

2. Microsoft Certification Authority in Enterprise mode (more details at Microsoft TechNet):

- Enrollment Agent Certificate Template
- Smartcard Logon Certificate Template

3. Third-party identity provider (Microsoft Azure, Okta, Ping Identity, Gemalto, etc.):

- This is where the user accounts should reside and be synchronized into the third-party SAML identity provider.
- The local AD is typically synchronized to the third-party IdP using an Active Directory Connector. Please consult with the provider on how to properly synchronize users.

4. Domain controllers (DC) must have domain controller certificates. The certificates on the DCs must support smart-card authentication. Certificates created using the Microsoft CA certificate template named "Domain Controller Authentication" supports smart-cards. Manually created DC certificates might not work.

5. Since SAML is a web-based authentication, it requires a browser, which is used to log in to the HTML5 portal and get application listing. The native Parallels Client for Windows is used to launch Remote Desktop Protocol (RDP) sessions.

6. For security reasons, the Enrollment Server (ES) must be a separate server and must not be installed on a Publishing Agent server. ES should be installed on a secure, standalone server that does not have any other components and roles installed.

Setting up the Windows Server side to comply with Parallels RAS SAML pre-requisites

Per the prerequisites above, configure Microsoft Certification Authority and certificate templates and add required user accounts. Detailed instructions are available in KB 124813.

Adding Parallels RAS Enrollment Server Agent

Install the Parallels RAS Enrollment Server Agent either manually or from the Parallels RAS Console.

- In Parallels RAS Console > Enrollment Servers > click “+” icon to add a new agent
- In the case of a manual ES setup (RASInstaller.msi > Custom), it is necessary to move the ES host registration key to the following folder: %installation_path%\Parallels\ApplicationServer\x64.
    - To export the registration key, open the Parallels RAS Console > ES > Tasks > Export registration key > registration.crt (remote pushing does this automatically)

In the Paralells RAS Console **> Enrollment Servers > AD Integration** tab, specify the CA and user accounts for Enrollment agent and NLA user you configured and apply the changes.

Final checks

Make sure the Enrollment Agent server status is OK.

Switch to AD Integration tab and click on Validate AD Integration settings. Make sure that all checks are passed.

Note: Ensure usernames are specified in UPN format

Azure side configuration

Here we need to create a generic SAML app.

1. Sign in to the Azure Portal and head to Azure Active Directory **>** **Enterprise applications >** create a new application by clicking on the appropriate button. Specify its name and click **Add**.

2. Select **Non-gallery application**, specify a name and click **Add** to create the application.

3. In the created application's blade, add users required to use SAML SSO. This can be done at the **Users and groups** pane.

Configuring Azure application to work with Parallels RAS

1. In the Azure Portal, open the SAML application blade and switch to **Single Sign-on** pane **> SAML**

2. At section 3 **SAML Signing Certificate**, copy the App Federation Metadata URL.

Note: For manual configuration, you can download Certificate (Base64) and Federation Metadata XML.

3. Open Parallels RAS Console **> Connection > SAML** tab **>** click **Add**

4. In the opened **Add Identity Provider** wizard, import metadata from the file or specify its URL. Choose an HTML5 Theme to associate the IdP with.

5. On the next page, the details about the certificate and logon/logout URLs should be auto-populated. If everything is correct, click **Finish**.

Note: Check "Allow unencrypted assertion" if you did not configure it in Azure.

6. Right-click on the IdP you just created **> Properties > SP** tab. Make sure that external **FQDN** or **public IP** specified in the **Hosts** field. Take a note of this information.

7. Switch back to the SAML application in the Azure portal. Specify the values at section #1 **Basic SAML Configuration** according to the SP tab in the Parallels RAS Console:

8. Configure attributes to match the IdP users with AD users. For instance, you may use Azure AD Connect to match users via **Immutable ID** as follows:

In AD, create an attribute:

Name	ImmutableID
Source	attribute
Source atrribute	user.onpremisesecurityidentifier

Further information is available at docs.microsoft.com

In our example, since this is the lab environment, we just use a custom attribute to match email address with the following setup:

- In Azure Portal > SAML app > Single Sign-On Open section #2 “User Attributes & Claims"
- Copy “claim name” of "user.userprincipalname" value:

- In the Parallels RAS Console’s **Add Identity Provider** window, switch to the Attributes tab and add a new one called **Custom**. Enable it and apply the settings.

Testing connectivity

1. Open the HTML5 Portal page in your web browser.

Note: Use the theme you associated with the SAML app.

2. If everything is correct, you will be immediately redirected to login.microsoft.online. Proceed with sign in.